The Division Algorithm

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \le r < d$, such that $a = dq + r$.

e.g. 12 is an integer & $5 \in \mathbb{Z}^+$ then

$12 = 5 \times 2 + 2$, here $0 \le r = 2 < 5$ & $q = 2, r = 2$ are unique.

The Euclidean ~~mel~~ algorithm

This algorithm is an efficient method for computing the GCD of two integers by using successive division algorithm until remainder becomes zero.

Ex. Find ~~GDt~~ GCD(91, 287)

By division algorithm,

$$287 = 91 \cdot 3 + 14$$

Any divisor of 91 and 287 must also be a divisor of $287 - 91 \cdot 3 = 14$. Hence, the greatest common divisor of 91 and 287 is the same as the GCD of 91 and 14.

Next, divide 91 by 14 to obtain

$$91 = 14 \cdot 6 + 7$$

Because any divisor of 91 & 14 also divides $91 - 14 \cdot 6 = 7$

$\therefore$ GCD(91, 14) = GCD(14, 7)

Continue by dividing 14 by 7, $14 = 7 \cdot 2$

$\therefore$ GCD(14, 7) ~~= GCD(7, 0)~~ = 7

$\therefore$ GCD(91, 287) = GCD(14, 91) = GCD(7, 14) = 7.